ISSN 1561-5359. Штучний інтелект, 2017, № 3-4

УДК 004.93

К.В. Колесніков, Б.П. Ободовський
Черкаський державний технологічний університет, Україна
бул. Шевченка, 460, м. Черкаси, 18000

ВИДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА МЕТОДИ ЇХ ОЦІНКИ

K.V. Kolesnikov, B.P. Obodovscky
Cherkassy state university of technology, Ukraine
460, Shevchenko blvd., Cherkasy, 18000

TYPES OF BIOMETRIC AUTHENTICATION AND METHODS OF THEIR EVALUATION

Біометрія дає альтернативу для персональної автентифікації: біологічні характеристики людини унікальні і можуть бути використані, щоб відрізняти одну особу від іншої. Біометрія - це автоматичні методи ідентифікації особи або підтвердження особистості на основі фізіологічної чи поведінкової характеристики. Приклади фізіологічних характеристик включають геометрію рук або відбитка пальця, особові риси та зображення радужної оболонки. Поведінкові характеристики - це риси, які вивчаються або набуваються. В роботі запропоновано загальний огляд біометричних систем на основі наявних технологій, методи застосування датчиків розпізнавання відбитків пальців та оцінки належних характеристик. Для тестування біометричних характеристик датчиків використано два індекси: FAR (false acceptance rate) та FRR (false retry rate).

Ключові слова: біометрія, автентифікація, безпека користувача, системи розпізнавання.

Biometrics provides an alternative to personal authentication: human biological characteristics are unique and can be used to distinguish one person from another. Biometrics are automatic methods for identifying a person or confirming a personality based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand geometry or fingerprint, personality traits, and iris image. Behavioral characteristics are the features that are studied or acquired. In the paper a general review of biometric systems is proposed based on available technologies, methods of using fingerprint sensors and assessment of proper characteristics. To test the biometric characteristics of the sensors, two indices are used: FAR (false acceptance rate) and FRR (false retry rate).

Key words: biometrics, authentication, user safety, recognition systems.

Вступ

Сьогодні більшість інформаційних систем надають користувачеві додаткові послуги, нехтуючи дуже важливим фактором: безпекою. Наприклад, потрібно запам'ятати багато паролів для доступу до банківського рахунку в Інтернеті або до поштової скриньки. Стандартні системи автентифікації, що базуються на імені користувача та паролі, не можуть забезпечити відповідний рівень захисту для переданої інформації. На жаль, цей механізм автентифікації не досконалий: хтось може незаконно знати та відтворювати секретну інформацію, яка повинна гарантувати лише доступ конкретної особи. Безпека повинна бути основним пунктом будь-якого програмного забезпечення, що стосується особистої інформації. Біометрія забезпечує альтернативний варіант особистої автентифікації: біологічна характеристика людини є унікальною і може бути використана для того, щоб відрізняти одну особу від іншої.

В роботі запропоновано загальний огляд біометричних систем та основних доступних технологій, а також аналіз тестування описаних характеристик датчиків розпізнавання відбитків пальців. Було використано два індекси, FAR (помилкова частота прийняття) та FRR (помилкова ставка відхилення).

© К.В. Колесніков, Б.П. Ободовський

Актуальність біометрії.

Кожна система автентифікації може вважатися валідною, якщо виконуються два наступні етапи:

- автентифікація цифрової ідентичності користувача;
- надання прав на виконання бажаної дії.

Автентифікація цифрової ідентичності користувача класифікується за допомогою трьох наступних підходів:

- якщо користувач знає пароль, то він є правильною людиною;
- якщо користувач має попередньо встановлений токен (магнітний значок чи смарткартку), то він є правильною людиною;
- система порівнює біометричні характеристики користувача з попередньо зареєстрованими значеннями, шаблоном, що дозволяє отримати доступ лише тоді, коли визначена характеристика відповідає шаблону, що зберігається в системі.

Найпоширеніші системи автентифікації використовують перший та другий підхід (або їх комбінацію) для реалізації розпізнавання користувача. Ці типи систем можуть бути легко порушені, просто викрадаючи токен або знаючи пароль. Ці два підходи потребують, щоб користувач пам'ятав або носив з собою "щось", що містить необхідну інформацію для автентифікації. Замість третього підходу користувачеві немає необхідності щось запам'ятовувати: вся інформація, необхідна для автентифікації, належить користувачеві. Фізичні та поведінкові характеристики користувача (як геометрія обличчя, райдужна оболонка ока та сітківка, відбитки пальців, голос, каліграфія тощо) є основою біометричних систем. Біометрична ідентифікація має перевагу – гарантований доступ буде забезпечено тільки тим, хто надає правильні фізичні характеристики. Біометрична система базується на біометричній характеристиці, яку неможливо викрасти.

Біометрична система, що використовує цифрові технології, може бути використана двома різними способами:

- режим ідентифікації: користувач ідентифікується базою даних про людей, відомих системі.
- режим автентифікації: користувачі оголошують свою особу, і система перевіряє це.

Біометрична система являє собою автоматичний пристрій для ідентифікації або автентифікації особистої ідентичності з використанням його біологічних характеристик. База даних, яка містить цифрове представлення (шаблон) біометричної характеристики, може бути централізованою або розподіленою.

У системі автентифікації виконуються дві різні фази.

Фаза реєстрації: виконується для введення біометричної характеристики в системну базу даних. На цій фазі виконуються три конкретні операції: введення біометричних характеристик, виведення цифрового біометричного представлення та зберігання шаблонів у базі даних.

Фаза перевірки: вона виконується кожного разу, коли користувач повинен бути автентифікований для доступу до системи. Три операції виконуються: введення біометричних характеристик, виведення біометричних цифрових представлень, порівняння біометричних характеристик та шаблонів, раніше створених на етапі введення.

Методи оцінки продуктивності.

Виконання біометричної системи можна оцінити, враховуючи наступні основні значення:

- розмір бази даних;

 © К.В. Колесніков, Б.П. Ободовський

- швидкість відповіді системи;
- точність розпізнавання користувачів.

Розмір шаблону, який використовує смарт-карту для зберігання, є основним питанням вибору типу біометричних технологій. Час, який використовується системою для прийняття рішення, є фундаментальним, особливо в програмах у режимі реального часу. Точність визнання є найважливішою характеристикою біометричних систем розпізнавання, оскільки вона визначає системну безпеку. Розпізнавання оцінюється за допомогою двох показників помилок: FAR, відсоток визнаних самозванців та FRR, відсоток відхилених зареєстрованих користувачів. Ці два відсотки завжди обчислюються: для кожної FAR є відносна FRR (Рис. 1).

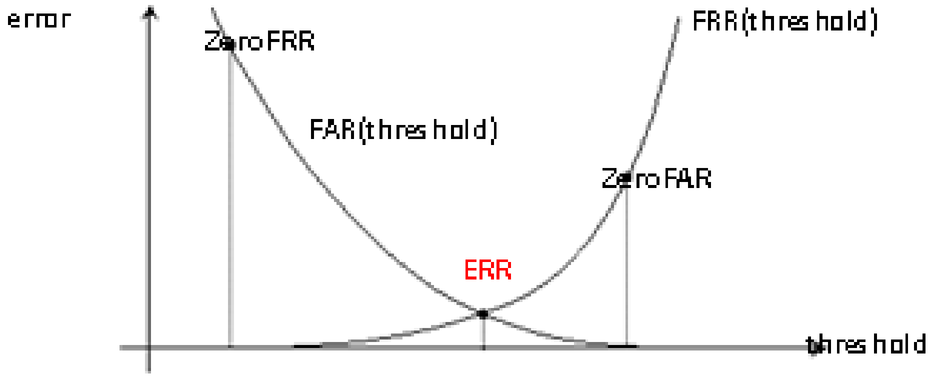


Рис. 1. Типовий графік відношення FAR і FRR біометричної системи.
Точка, де FAR дорівнює FRR, є точкою EER. Zero FAR - значення FRR, коли FAR дорівнює нулю і навпаки.

У ідеальній біометричній системі ці відсотки були б рівними нулю. На жаль, ідеальної системи не існує, тому доведеться досягати компромісу між значеннями FAR та FRR: більшість програм намагаються утримати ці два індекси якомога нижче. Для оцінки глобального відсотка помилки системи використовується EER (Equal Error Rate), визначений як відсоток, коли FAR та FRR рівні. За допомогою біометрії слід визначити метрику, щоб встановити близькість порівняння зі значенням відсічення: тільки якщо значення, пов'язане з вимірюваною біометричною характеристикою, подолає граничне значення, то система визнає ідентичність користувача. Системний адміністратор, коли встановлюється граничне значення, вибирає компроміс серед імовірності помилкових прийомів (що дозволяють отримати доступ незареєстрованим особам) та помилкових відмов (відмову в доступі правильній особі).

Ергономічність біометричних характеристик

Наступна таблиця 1 показує найбільш поширені фізіологічні та поведінкові характеристики людини, що використовуються для реалізації біометричної системи.

Ці характеристики мають такі специфічні властивості:

- універсальність: кожна людина повинна мати характеристику, яка використовується системою;
- невідповідність: характеристика повинна бути розрізненою – дві людини не повинні бути рівними з точки зору однієї характеристики;
- продуктивність: оптимальний EER повинен бути індивідуалізований;

- надійність: характеристики не повинні змінюватися або змінюватися протягом життя людини;
- прийнятність: фаза ведення не повинна бути нав'язливою, і система повинна бути зручною для користувачів.

Таблиця 1. Порівняння біометричних технологій

Біометрична технологія	**Універсаль-ність**	**Невідповід-ність**	**Надій-ність**	**Продуктив-ність**	**Прийнят-ність**
Геометрія обличчя	Висока	Низька	Посередня	Низька	Висока
Термограма обличчя	Висока	Низька	Посередня	Низька	Висока
Відбиток пальців	Посередня	Висока	Висока	Висока	Посередня
Геометрія руки	Посередня	Посередня	Посередня	Посередня	Посередня
Райдужна оболонка	Висока	Висока	Висока	Висока	Низька
Сітківка	Висока	Висока	Посередня	Висока	Низька
Голос	Посередня	Низька	Низька	Низька	Висока
Почерк	Низька	Низька	Низька	Низька	Висока

Біометричні методи

Аналіз принципів біометрії показав, що кожна технологія має свої переваги та недоліки.

Геометрія обличчя та термограмм облич. Біометричні системи, які використовують розпізнавання обличчя, базуються на відстані між атрибутами обличчя та їхньою формою. У фазі доступу до системи здійснюється введення і подання системі особистої картини для порівняння з зображенням, що зберігається в базі даних (Рис. 2а). Система розпізнавання геометрії обличчя дуже чутлива до варіацій підсвічування, до різних позицій обличчя та виразів.

Термограма базується на моделі інфрачервоного зображення обличчя. Як недолік можна відмітити, що термограма обличчя чутлива до емоційного стану та стану здоров'я людини.

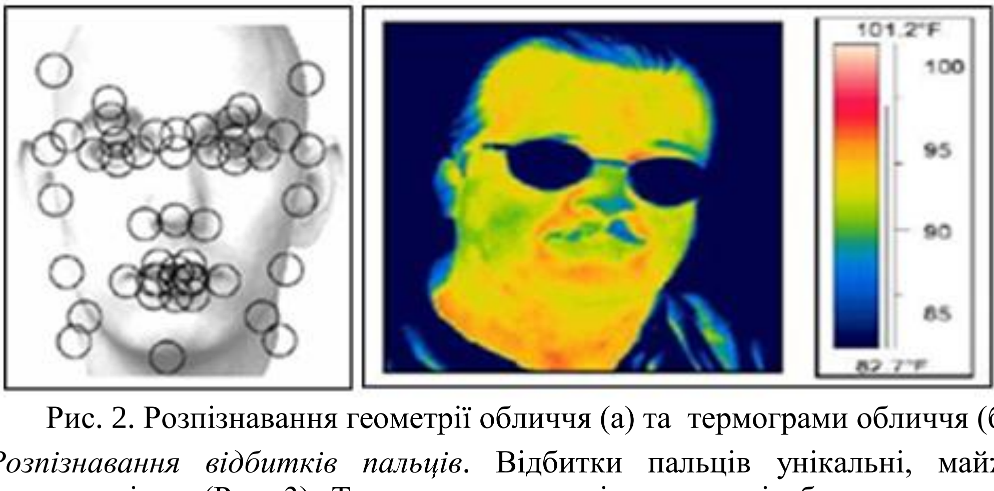


Рис. 2. Розпізнавання геометрії обличчя (а) та термограми обличчя (б).

Розпізнавання відбитків пальців. Відбитки пальців унікальні, майже не змінюються з віком (Рис. 3). Також ця технологія має певні обмеження: надмірно волога чи суха шкіра може погіршити продуктивність системи, або коли відбитки пальців пошкодженні або мають шрами.

 © К.В. Колесніков, Б.П. Ободовський

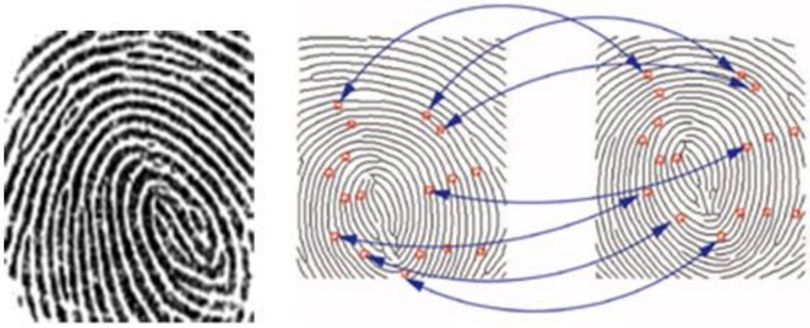


Рис. 3. Відбиток пальців, отриманий оптичним сканером (а) та відповідністю між двома відбитками пальців з мікро характеристиками (б).

Геометрія рук. Форма та розміри рук можуть бути використані в якості відмінних характеристик. Системи розпізнавання геометрії рук (рис. 4а) мають багато переваг, що стосуються відбитків пальців: для зберігання шаблонів потрібно менше місця, вся система є більш зручною. Результат залежать від погодних умов або від чистоти руки, а форма руки не є постійною протягом життя. Нарешті, реальною проблемою є великий розмір датчика руки (рис. 4б). Через незручність використання, складність обладнання, погану точність, так само, як і розпізнавання сітківки ока, цей метод не дуже ефективним.



Рис. 4. Сканування геометрії рук (а) та сканер геометрії рук (б).

Райдужна оболонка ока. Райдужна оболонка є унікальною для людського тіла. Навіть майже ідентичні близнюки мають різні райдужки. Ця технологія використовує певні сенсори для сканування та не вимагає контакту між оком суб'єкта та біометричним сканером (рис. 5а). Шаблон вимагає лише кілька байтів для зберігання, і система працює, навіть якщо людина носить окуляри.

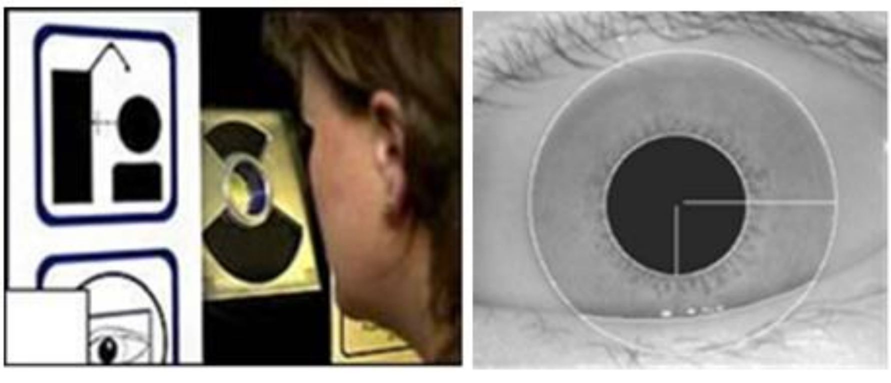


Рис. 5. Сканер (а) та сегментації райдужки (б).

© К.В. Колесніков, Б.П. Ободовський

Розпізнавання каліграфії. Ця техніка базується на характеристиці, що кожна людина має унікальний стиль для написання. Проблема в тому, що два твори однієї і тієї ж людини ніколи не є абсолютно ідентичними. Існують два підходи до розпізнавання каліграфії: статичні та динамічні. Динамічний метод враховує прискорення, швидкість і тиск при написанні для підвищення точності розпізнавання.

Розпізнавання голосу. Розпізнавання голосу вважається найменш точною технологією, воно може забезпечити безпечний доступ до інформації через телефонні лінії. Розпізнавання голосу може бути залежним від тексту або незалежним від тексту: у першому випадку користувач повідомляє заздалегідь визначену фразу; у другому випадку користувач просто щось говорить. Проблема цієї технології полягає в тому, що шум навколишнього середовища може сильно знизити продуктивність. Близнюки та брати майже не відрізняються. Також відсотки помилок є високими серед різних людей.

Вибір біометричної технології.

Біометричні технології гарантують безпечне розпізнавання користувачів у різних галузях, що в основному відносяться до:

- управління фізичними доступом: наприклад в тих областях, де важливо знати, хто входить і хто виходить (наприклад, в офісах, лікарнях, в'язницях тощо);
- логічний контроль доступу: це доступ через комп'ютерні мережі, стільникові телефони до зарезервованих даних або послуг, де важлива безпека (електронний банкінг, пошта та ін.);

Вибір біометричної технології зазвичай здійснюється за такими факторами (табл.2):

- необхідний тип рішення;
- середовище, де буде використовуватися біометрична система;
- потрібний рівень безпеки.

Таблиця 2- Основні характеристики запропонованих технологій

Біометрична технологія	**FAR (%)**	**FRR (%)**	**Вартість**	**Розмір шаблону, (Байт)**	**Розуміння користувачем**
Форма обличчя	10-20	0.001-1	Середня	<10	Високе
Форма долоні	1-10	1	Середня	<10	Посередне
Райдужна оболонка	1-10	~0	Висока	512	Низьке
Сітківка	1	0.01	Дуже висока	512	Низьке
Голос	10-20	2-5	Низька	1500	Високе
Каліграфія	3-10	1	Середня	1500	Високе
Відбиток пальця	3-7	0.0001-0.001	Середня	300÷1200	Посередне

Датчик розпізнавання відбитків пальців.

У системі автентифікації відбитків пальців найважливішою частиною є біометричний датчик, що складається з трьох модулів: UIM, PM та AM (Рис. 6).

© К.В. Колесніков, Б.П. Ободовський

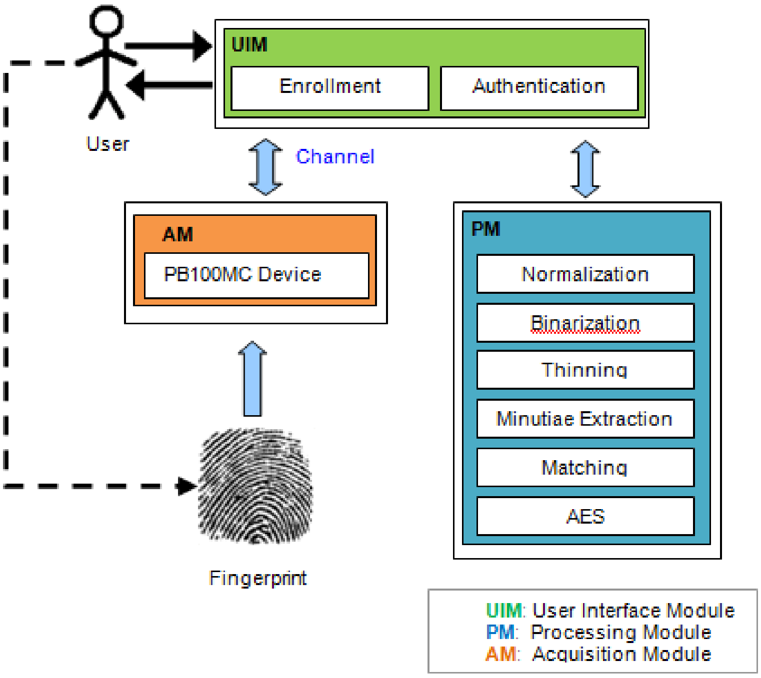


Рис. 6. Три модулі датчика розпізнавання відбитків пальців.

UIM: модуль користувальницького інтерфейсу. UIM - це модуль, спеціально розроблений для забезпечення необхідного інтерфейсу для доступу до функцій реєстрації та автентифікації, наданих біометричним датчиком. На етапі реєстрації наступні кроки можуть бути індивідуалізованими:

- відбиток користувача зафіксований сканером PB100MC [4].
- зображення відбитка надсилається до PM.
- створюється біологічний шаблон.
- шаблон зашифровується за допомогою алгоритму AES і зберігається в системній базі даних.

Натомість, у фазі автентифікації, можна індивідуалізувати наступні кроки:

- відбиток пальця користувача в реальному часі знімається сканером;
- зображення прямого відбитка пальця та зашифрованого біологічного шаблону надсилаються до PM;
- зображення обробляється PM, а деталі витягуються і збігаються з розшифрованим біологічним шаблоном, присутнім у системній базі даних;
- якщо результат порівняння є позитивним (якщо користувач автентифікується), йому надається доступ.

PM: модуль обробки. PM - це модуль, який реалізує всі розробки, необхідні для зчитування відбитків пальців біометричного шаблону. Реалізовані наступні шість завдань: нормалізація, бінаралізація, розрідження, вилучення мікроелементів, шифрування / розшифровка цифрових шаблонів та відповідність.

AM: модуль введення. AM керує сканером відбитків пальців та захопленням відбитків пальців. Він складається з пристрою Precise Biometrics PB100MC. В рамках стандартного інтерфейсу, наданого Bio API [5][6]. Перш за все шаблон користувача повинен бути створений. Характеристики, отримані зразками, складаються з шаблону, який буде запам'ятовуватися біометричною системою.

Аналіз розпізнання

Продуктивність біометричної системи була розрахована через FAR та FRR (табл. 3). Ідеальний датчик автентифікації матиме значення FAR та FRR, рівними нулю, замість цього в реальній системі, зареєстровані користувачі, відхиляються системою (помилкові відмови), а користувачі, які не записані, приймаються (помилкові прийняття). Таким чином, значення FAR і FRR не дорівнюють нулю. Для оцінки цього індексу та для їх оптимального вибору було проведено різні тести на наборі 352 відбитків пальців 88 користувачів, зафіксованих за допомогою сканера PB100MC.

Таблиця 3. Значення FAR та FRR з урахуванням змінної мінімального відсоткового співвідношення мінімальних значень та 2, 3 та 4 відбитків пальців для автентифікації користувача.

Ефективність датчика	**85%**		**90%**		**93%**		**95%**		**97%**	
Кількість відбитків пальців	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**
2	6,35	3,13	2,99	5,21	1,68	7,29	1,07	8,33	0,98	11,46
3	3,93	8,33	1,71	14,58	1,12	17,71	0,78	22,92	0,71	26,04
4	2,16	25,00	0,99	32,29	0,87	40,63	0,60	46,88	0,41	52,08

Висновки

Біометрія дозволяє автоматичному датчику автентифікації користувача використовувати свої фізіологічні чи поведінкові характеристики, що підвищують рівень безпеки системи. Біометричний датчик є чинним альтернативним відношенням до "звичайних" систем автентифікації на основі традиційних методів автентифікації (наприклад, пароля та PIN-коду). Сучасні біометричні датчики є менш дорогими, а також більш мініатюрними, що дозволяє легше розповсюджувати біометричні системи автентифікації. Крім того, біометрія є ефективною стратегією захисту приватності. Нарешті, біометричні датчики, в майбутньому, можуть бути використані майже в кожній транзакції, яка потребує безпечної особистої автентифікації.

Література

1. Болл Р. Руководство по биометрии / Р.М. Болл, Дж.Х. Коннел; [пер. с англ. под ред. Н. Агапова]. – М.: Техносфера, 2007. – 368 с.
2. Лакин Г. Биометрия / Лакин Г.Ф. – М.: Высшая школа, 1990. – 352 с.
3. Кауненко С.І., Колесніков К.В. Методи ідентифікації людини в інформаційних системах ISDMCI’2012: Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта: Материалы международной научной конференции.- Херсон-Євпаторія ХНТУ,2012, 566с., С. 164-167.
4. Precise Biometrics // [Електр. Ресурс]. – Режим доступу: https://precisebiometrics.com/
5. An emerging biometric API industry standart // [Електр. Ресурс]. – Режим доступу: http://ieeexplore.ieee.org/document/820046/
6. BioAPI Specification Version 1.1 // [Електр. Ресурс]. – Режим доступу: http://xml.coverpages.org/BIOAPIv11.pdf

Literatura

1. Boll R. Rukovodstvo po biometrii / R.M. Boll, Dg.H. Konnel; [per. s angl. pod red. N. Agapova]. – M.: Tehnosfera, 2007. – 368s.
2. Lakin G. Biometria / Lakin G.F. – M.: Vusshay shkola, 1990. – 352 s.

 © К.В. Колесніков, Б.П. Ододовський

3. Kaunenko S.I., Kolesnikov K.V. Metody identifikazii ludyny v informaziynyh systemah ISDMCI’2012: Intellektualnye systevy prinatia resheniy I problemy vychislitelnogo intellekta: Materialy mezhdunarodnoy nauchnoy konferenzii.- Herson-Evpatoria HNTU,2012, 566s., s. 164-167.
4. Precise Biometrics // [Elektr. Resurs]. – Rezhym dostupu: https://precisebiometrics.com/
5. An emerging biometric API industry standart // [Elektr. Resurs]. – Rezhym dostupu: http://ieeexplore.ieee.org/document/820046/
6. BioAPI Specification Version 1.1 // [Elektr. Resurs]. – Rezhym dostupu: http://xml.coverpages.org/BIOAPIv11.pdf

RESUME

K.V. Kolesnikov, B.P. Obodovscky

Types of biometric authentication and methods of their evaluation

Biometrics is a complex of methods and technologies for automatic identification of an individual by anatomical, physiological or behavioral features.

The biometry allows to use physiological or behavioral characteristics in an automatic authentication sensor, which increases the security of the system. A biometric sensor is an alternative to "ordinary" authentication systems that were based on traditional methods (such as a password and a PIN). Current biometric sensors are less expensive and more tiny, that makes implement of biometric authentication systems easier. In addition, biometrics is an effective privacy protection strategy. In the future, biometric sensors can be used in almost every transaction that requires secure of personal authentication.

This article provides a general overview of biometric systems and basic available biometric technologies such as face geometry and thermograms, fingerprint recognition, hand geometry, eye iris, calligraphy recognition and voice recognition. The main problem in the field of biometrics is the accuracy of recognition, because the more accurate the system - the more it is safer. In some cases, the speed of a system can certainly be more useful, but usually, it is precisely the security and precision of the system that is of the utmost importance. That is why the greatest attention was paid to the analysis of the characteristics of fingerprint sensor sensors using two indices, FAR (false reception frequency) and FRR (false rate of deviation).

As a result of data processing, results were obtained that can be seen as changing the accuracy and efficiency of the fingerprint sensor when the user uses more than one of his own prints for authentication.

Надійшла до редакції 28.10.2017